REMARKS

Introduction

This Reply is in response to the Office Action of June 23, 2008. Reconsideration of this application in view of the following remarks is respectfully requested.

Drawings

The originally filed drawings in the patent application were objected to as being difficult to read. Applicant is therefore submitting formal drawings herewith.

The Rejections of Claims 1-19

In the Office Action, claims 1-19 were rejected under 35 U.S.C. §102(e) as being anticipated by Zheng (US 6396928). These rejections are respectfully traversed.

Summary of Applicant's Invention

Applicant's invention relates to identity-based-encryption (IBE) signcryption systems for signing and encrypting data. In an IBE system, the sender and the recipient each have IBE public and IBE private keys. A sender in an IBE system may generate a given recipient's IBE public key based on known rules. For example, a message recipient's email address or other identity-based information may be used as the recipient's public key, so that a sender may create the IBE public key of a recipient by simply determining the recipient's email address. In a signcryption system, signing and encrypting are performed in a single process. Unlike conventional signcryption systems, applicant's system supports IBE signcryption operations.

With the applicant's IBE signcryption technique, a sender signs and encrypts a message using an IBE private key of the sender and an IBE public key of the recipient (see, e.g. step 54 of FIG.5). The encrypted message (known as ciphertext C) is then sent anonymously to the recipient (see, e.g. step 56 of FIG.5). The recipient uses the recipient's IBE private key to decrypt ciphertext C to produce the original message, the sender's IBE public key which identifies the sender, and the sender's IBE signature of the message (step 62 of FIG. 5). After the decryption process, the recipient or a third-party can perform signature verification to verify that the message was signed by the sender. The signature verification process is performed using the decrypted original message, the message signature, the sender's IBE public key (steps 64, 66, 68 of FIG. 5). The decryption and verification is thus a two-step process.

Claims 13-17

Claim 13 is directed toward a method of signing and encrypting a message M. The method of claim 13 involves obtaining an identity-based-encryption (IBE) private key of a user. The IBE private key is then used to compute a commitment to a secret value and a corresponding decommitment. A symmetric key is used to encrypt the commitment or the decommitment. The language of claim 13 makes it clear that the symmetric key is based on the IBE private key.

In the Office Action, claim 13 was rejected as being anticipated by Zheng. In making this rejection, it was suggested that the passages in column 13 of Zheng disclose obtaining an identity-based encryption (IBE) private key of a user and using the IBE private key to compute a commitment and decommitment.

However, the Zheng scheme in column 13 is based on SCS1 encryption. As set forth in the table at the top of column 10, SCS1 encryption involves the use of cryptographic parameters that include secret key x_a and public key y_a. In column 9, lines 6-30, Zheng makes it clear that Alice's secret key x_a is used in computing Alice's public key y_a. Alice selects the secret key x_a from [1..q]. This selected value of x_a is then used in computing Alice's public key $y_a = g^{x_a}$. Because Alice's public key y_a is determined by this equation from the selected value of x_a, y_a is not associated with an identity. Alice's public key y_a thus does not form an identity-based encryption (IBE) public key. The corresponding value of x_a therefore does not serve as an IBE private key.

Accordingly, there is nothing in Zheng that shows or suggests obtaining an identity-based encryption (IBE) private key as required by claim 13. There is also nothing in Zheng that shows or suggests using an IBE private key to compute a commitment and decommitment. Claim 13 is therefore not anticipated by Zheng.

Moreover, claim 13 makes it clear that the symmetric key that is used to encrypt the commitment or the decommitment is based on an IBE private key. In the Office Action, it was suggested that Zheng discloses use of a symmetric key that is based on an IBE private key to encrypt a commitment or decommitment in FIGS. 3 and 4 and at column 13, lines 34-67. However, this portion of Zheng merely discloses the use of an SCS1-based cryptographic scheme. This scheme does not compute a commitment or decommitment from an IBE private key, let alone encrypt a commitment or decommitment using a symmetric key formed from an IBE private key. There is simply no symmetric key in Zheng that is formed from an IBE private key.

Claim 13 is therefore not anticipated by Zheng for these additional reasons. Claims 14-17 depend from claim 13 and are patentable because claim 13 is patentable.

Claims 1-12 and 18-19

In the Office Action, claims 1 and 18 were rejected as being anticipated by Zheng.

Claim 1 is directed towards an identity-based-encryption (IBE) signcryption method in which a sender signs and encrypts a message M for a recipient. The method of claim 1 involves digitally signing and encrypting a message M in a signcryption operation using an IBE private key of the sender SK_A and an IBE public key of the recipient ID_B that is based on the recipient's identity to generate a ciphertext C that is a signed and encrypted version of the message M. Claim 1 also involves sending the ciphertext C to the recipient anonymously, so that an attacker cannot deduce the authorship of the message from the ciphertext C. According to the language of claim 1, the recipient decrypts the ciphertext C using an IBE private key SK_B of the recipient that corresponds to the IBE public key ID_B. This produces an unencrypted version of the message M and an IBE public key of the sender ID_A that corresponds to the IBE private key SK_A. After the ciphertext has been decrypted by the recipient, signature verification is performed in an operation that is separate from the decryption of the ciphertext. The signature verification operation uses the decrypted message M and the IBE public key of the sender ID_A to prove that the sender signed the message M.

As described in connection with claim 13, Zheng discloses cryptographic schemes in which public keys are computed from selected secret keys and are therefore not associated with identities. As a result, Zheng does not show or suggest the use of identity-based encryption (IBE) in performing signcryption operations as required by claim 1.

In particular, there is nothing in Zheng that shows or suggests digitally signing and encrypting a message M in a signcryption operation using an IBE private key of a sender SK_A and an IBE public key of a recipient ID_B as required by claim 1. There is also nothing in Zheng that shows or suggests decrypting ciphertext C using an IBE private key SK_B of a recipient that corresponds to an IBE public key ID_B. Zheng also does not show or suggest a signature verification operation that uses an IBE public key of a sender ID_A to prove that a sender signed a message M. In view of these shortcomings, Zheng fails to anticipate claim 1 and is therefore allowable. Claim 18 is allowable for at least the same reasons that claim 1 is allowable.

Claims 2-12 depend from claim 1 and are patentable because claim 1 is patentable. Claim 19 depends from claim 18 and is patentable because claim 18 is patentable.

Conclusion

The foregoing demonstrates that claims 1-19 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

Respectfully submitted,

Date: October 21, 2008

/G. Victor Treyz/
G. Victor Treyz
Reg. No. 36,294
Attorney for Applicant
Customer No. 36532